KOREAN PATENT ABSTRACTS

(11)Publication number: **10-2001-0025209 A**

(43)Date of publication of application: **06.04.2001**

(51)Int. Cl.

G06F 17/00

(21)Application number: **10-2000-0061970**

(22)Date of filing: **20.10.2000**

(71)Applicant: **INTERPIAWORLD CO., LTD.**

(72)Inventor: **KO, JIN SEON**

---

(54) METHOD FOR FILTERING INAPPROPRIATE CONTENT AND RECORDING MEDIUM STORING FILTERING PROGRAM

(57) Abstract:

PURPOSE: A method for filtering an inappropriate content and a recording medium storing a filtering program are provided to minimize filtering error of the inappropriate content, configure a search algorithm for minimizing the error and provide log file search function for the filtering from a remote place via internet.

CONSTITUTION: An inappropriate content filtering service provider performs real-time analysis and accumulation of the inappropriate content using an inappropriate content search robot and constructs an inappropriate content data base. A user logs on the web server of the service provider via internet and inputs personal information and information for utilizing the filtering service requested by the service provider. The service provider constructs a member information data base based on the input information. The user receives a program for filtering the inappropriate content, installs the program in a user's computer and drives the program for setting function of the inappropriate content filtering and a remote management. If the user executes the inappropriate content filtering function of the program, the service provider provides information of a remote inquiry about use of an inappropriate content, member management and the inappropriat content filtering to the user.

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl. 6
G06F 17/00

(11) 공개번호 10-2001-0025209
(43) 공개일자 2001년04월06일

(21) 출원번호 10-2000-0061970
(22) 출원일자 2000년10월20일

(71) 출원인 주식회사 인터피아월드 고진선
서울특별시 강남구 대치4동 896-302
(72) 발명자 고진선
서울특별시송파구잠실1동주공아파트30동404호
(74) 대리인 제갈혁
류완수
이광복
조진수

심사청구 : 있음

(54) 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법및 이를 구현할 수 있는 프로그램이 수록된 컴퓨터로 읽을수 있는 기록매체

요약

본 발명은 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법 및 이를 구현할 수 있는 프로그램이 수록된 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다. 본 발명은, (a)사업자가 유해 정보 검색 수단을 이용하여 유해 정보를 실시간으로 분석 및 수집하고, 유해 정보를 웹 서버에 연동되는 유해 정보 데이터베이스로 구축하는 단계; (b)사업자가 이용자의 입력 정보를 웹 서버에 연동되는 회원 정보 데이터베이스로 구축하는 단계; (c)사업자가 이용자에게 유해 정보를 차단시킬 수 있는 유해 정보 차단 프로그램을 제공하면, 이용자는 유해 정보 차단 프로그램을 이용자의 PC에 탑재하는 단계; (d)이용자가 유해 정보 차단 프로그램을 구동시켜 상기 이용자 PC의 유해 정보 차단 및 원격 관리 여부를 설정하고, 유해 정보 차단 기능을 실행시키는 단계; 및 (e)사업자는 사업자의 서버에 접속한 이용자에게 유해 정보 사용에 대한 원격 조회 정보, 회원 관리 정보 및 유해 차단 관련 정보를 제공하는 단계;를 포함하여 진행하는 것을 특징으로 한다. 본 발명에 따르면, 유해 정보의 원격 관리가 가능하고, 학습 사이트 및 유익한 사이트까지 차단시키는 오류를 방지함과 동시에 유해 정보의 실시간 검색이 가능하다.

대표도

도1

색인어

네트워크, 유해, 서비스, 프로그램, 기록매체

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 네트워크를 이용한 유해 정보 차단 서비스 사업 방법의 일실시예를 설명하기 위한 네트워크 구성도이다.

도 2는 본 발명에 따른 서비스 사업 방법의 유해 정보 차단 프로그램의 동작을 설명하기 위한 블럭도이다.

도 3은 본 발명에 따른 서비스 사업 방법의 이용자가 사업자의 서버에 접속하여 필요한 서비스 정보를 선택하는 과정의 일실시예를 나타내는 흐름도이다.

도 4는 본 발명에 따른 서비스 사업 방법의 사업자가 이용자에게 제공하는 원격 관리 리스트 웹 페이지의 일실시예이다.

도 5는 본 발명에 따른 서비스 사업 방법에서 유해 차단 프로그램 실행 과정의 일실시예를 나타내는 흐름도이다.

도 6은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 이용 정보 중 기록 보기를 선택하는 과정의 일실시예를 나타낸 흐름도이다.

도 7은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 인터넷 차단 기록 보기창의 일실시예이다.

도 8은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 인터넷 사용 기록 보기창의 일실시예이다.

도 9는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 일반 설정을 하는 과정의 일실시예이다.

도 10은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 프로그램 사용 제한창의 일실시예이다.

도 11은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 프로그램 시간 제한창의 일실시예이다.

도 12는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 개별 차단창의 일실시예이다.

도 13은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 설치, 업그레이드 및 삭제의 일실시예이다.

도 14는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 컴퓨터 검사창의 일실시예이다.

도 15는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 새로운 단어 목록창의 일실시예이다.

도 16 내지 도 18은 본 발명에 따른 서비스 사업자가 서버에 구축한 데이터베이스 구축도들이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야 종래기술

본 발명은 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법 및 이를 구현할 수 있는 프로그램이 수록된 컴퓨터로 읽을 수 있는 기록매체에 관한 것으로서, 보다 상세하게는 이용자가 인터넷을 통해 음란, 폭력, 마약등과 관련된 유해 사이트에 접속하는 것을 사전에 차단하고, 이용자는 사업자가 제공하는 사업자의 유해 정보 데이터베이스 서버를 이용함으로서 유해 정보에 대한 실시간 검색을 할 수 있고, 이용자가 사업자의 웹 서버에 접속하여 인터넷 사용 기록을 원격 조회할 수 있도록 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법 및 이를 구현할 수 있는 프로그램이 수록된 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

최근들어, 인터넷 인구 1,600만이 넘어설 정도로 생활의 일부가 되어버린 인터넷은 주 사용층인 청소년의 경우 30%가 스스로 컴퓨터 중독 증세가 있다고 밝히고 있고 청소년들이 인터넷을 통해 쉽게 접속할 수 있는 유해 사이트는 무려 15만 여 곳이나 되며 마약, 음란, 폭력등의 자극적인 내용들이 범람하는 유해 사이트가 계속 늘어나는 추세에 있다.

따라서, 청소년들의 유해 사이트의 접속을 차단하기 위한 프로그램이 개발되어 사용되고 있고, 상기와 같은 프로그램은 사용자에 의한 컴퓨터 설치 프로그램으로 인터넷 접속 통로를 감시하는 방법으로 동작하는 검열 소프트웨어의 범주 독립형 소프트웨어 (stand alone software) 위주의 개발이 이루어지고 있으며, 불건전 사이트 목록, 이용자 설정의 단어 및 목록을 이용한 제한 방식이 대부분이다.

일반적인 유해 정보 차단 방법은 유해 정보 차단 프로그램을 이용자의 컴퓨터에 탑재하여 음란, 마약, 도박, 폭력, 테러등 유해한 정보를 담고 있는 인터넷 사이트를 사전에 차단하는 방법이 대부분이다. 여기서, 상기 유해 정보 차단 프로그램은 일종의 필터링 소프트웨어로서 인터넷을 통한 유해 사이트 정보 목록을 갱신함으로서 유해 사이트에 대항하는 체계로 구성되어 있다.

그러나, 상기와 같은 유해 정보 차단 방법은 단어 검색에 의한 차단 방식의 경우 홈페이지 내에서 특정 유해 단어를 검색하는 방식으로 단어의 사용과 출현 빈도등으로 차단이 되며, 부분적인 단어를 검색하여 차단을 시킬 경우 유해 사이트가 아닌 사이트를 차단시키는 이른바 오/차단율이 매우 높은 문제점이 발생하게 된다. 예를 들어, SEX 라는 단어의 경우 이는 교육 사이트에서도 나올 수 있는 단어이기 때문에 유해한 단어를 검색하여 차단 시키는 방법에는 많은 오류와 한계가 있을 수 있다.

또한, 유해 정보 사이트 데이터베이스를 이용하는 방법은 웹 사이트의 해당 URL(uniform resource locator)을 유해 정보 차단 데이터베이스 서버에 의뢰를 통해 유해 사이트 여부를 결정하여 차단하는 방식으로, 유해 사이트의 데이터베이스화가 이루어져 있어야 하며, 이 방식을 이용할 경우 모든 사이트에 대한 URL을 서버에 의뢰하게 되므로 순간 접속량이 폭주할 경우 서버 과부하로 인해 서비스 장애가 발생하고, 매일 수시로 생겨나는 세계의 모든 유해 사이트에 대한 지속적인 데이터베이스화 작업이 이루어지지 아

니할 경우 신규 유해 사이트에 대한 정보 부재로 차단율이 낮아지게 되고, 수작업에 의한 유해 사이트의 검색은 신규 유해 사이트 검색에 한계를 가지게 되는 문제점이 있었다.

최근 정보 통신부와 정부가 인터넷 유해 환경에 대한 중요성을 인식하고 웹 사이트에 대한 등급제 인증 제도 및 기타 유해 사이트에 대한 제재 방침을 발표하기 시작하면서 많은 이용자 층과 인터넷 회선 사업자, 컴퓨터 보급 업체, 각급 기관 및 학교등에서 유해 정보 차단에 대한 수요가 급증하고 있는 추세이다.

따라서, 청소년의 무분별한 음란물 정보로 부터 무분별한 유출을 막고자 하는 부모와 교육 기관이 실질적 사용자층이므로 실질적인 사용자 측면을 고려한 유해 차단 기술 개발이 절실히 요구되고 있으며, 이를 토대로 본 발명을 착안하게 되었다.

발명이 이루고자하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 종래의 유해 정보 차단 방법이 단어 검색 방식에 있어 오/차단율이 매우 높고, 유해 정보 데이터 베이스 이용 방식에 있어 서버 과부하로 인한 서비스 장애가 발생하고, 지속적으로 데이터베이스 축적 작업이 이루어지지 않는 문제점등을 해결하고자 함에 있으며, 이를 위해 유해 사이트 검색/차단, 단어 검색 차단 및 유해 정보 데이터베이스 검색 차단 방식을 동시에 지원하여 유해 사이트 차단의 오/차단율을 최소화하고, 유해 정보 검색 로봇을 이용하여 신규 음란 사이트의 유해 정보 데이터베이스에 실시간으로 저장하여 신규 유해 사이트 검색에 대한 오/차단율을 최소화하기 위한 검색 알고리즘을 구현하고, 인터넷을 통한 원격지에서의 유해 정보 차단 로그 파일 검색 기능을 제공할 수 있는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법 및 이를 구현할 수 있는 프로그램이 수록된 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

발명의 구성 및 작용

전술한 목적을 달성하기 위한 본 발명은, 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법에 있어서, (a)사업자가 유해 정보 검색 수단을 이용하여 유해 정보를 실시간으로 분석 및 수집하고, 상기 유해 정보를 웹 서버에 연동되는 유해 정보 데이터베이스로 구축하는 단계; (b)상기 사업자의 서버에 이용자가 통신 네트워크를 이용하여 접속한 후, 상기 사업자가 요구하는 회원 정보 및 유해 정보 차단 서비스 이용에 관한 정보를 입력하면, 사업자는 이용자가 입력한 정보를 웹 서버에 연동되는 회원 정보 데이터베이스로 구축하는 단계; (c)상기 사업자가 사업자의 서버에 접속한 이용자에게 유해 정보를 차단시킬 수 있는 유해 정보 차단 프로그램을 제공하면, 이용자는 유해 정보 차단 프로그램을 이용자의 PC에 탑재하는 단계; (d)상기 이용자가 유해 정보 차단 프로그램을 구동시켜 상기 이용자 PC의 유해 정보 차단 및 원격 관리 여부를 설정하고, 유해 정보 차단 기능을 실행시키는 단계; 및 (e)상기 사업자는 사업자의 서버에 접속한 이용자에게 유해 정보 사용에 대한 원격 조회 정보, 회원 관리 정보 및 유해 차단 관련 정보를 제공하는 단계;를 포함하여 진행하는 것을 특징으로 한다.

이때, 상기 (a)단계의 유해 정보 검색 수단은 유해 사이트의 웹 페이지 본문 내용을 텍스트 언어로 변환하여 어구 분석 작업을 통해 상기 본문 내용과 링크된 웹 주소를 분류하고, 상기 링크된 웹 주소만을 데이터베이스에 기록하는 것이 바람직하다.

또한, 상기 유해 정보 검색 수단은 어구 분석된 본문 내용을 검색하여 유해 정보 사이트 판단시 자동으로 데이터베이스에 입력이 이루어지게 하는 것이 바람직하다.

여기서, 상기 (d)단계의 유해 정보 차단 기능을 실행시키는 단계는, (d1)이용자가 암호 인증 정보를 입력하는 단계; 및 (d2)이용자가 인터넷 사용 기록 보기 정보 설정, 프로그램 관리 정보 설정, 프로그램 사용 제한 정보 설정, 프로그램 제한 시간 정보 설정, 인터넷 사용 제한 정보 설정 및 유해 주소 차단 정보 설정 중 선택된 어느 하나 이상의 정보를 설정하는 단계;를 더 포함하여 진행하는 것이 바람직하다.

여기서, 상기 이용자는 인터넷 사용 기록 보기를 통하여 인터넷 사이트 차단 기록, 인터넷 사용 기록 및 날짜별 인터넷 사용 기록을 볼 수 있는 것이 바람직하다.

여기서, 상기 (d)단계의 원격 관리는 이용자가 최초 설정한 유해 사이트 정보 또는 사업자가 구축한 유해 정보를 기초로 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 유해 사이트를 방문하면 자동으로 사업자의 서버에 연동되는 회원 정보 데이터베이스로 유해 사이트 접속 시간 및 유해 사이트 주소가 저장되어, 상기 이용자가 인터넷 접속이 가능한 장소에서 사업자의 서버에 접속하여 이용자 컴퓨터의 유해 차단 기록을 볼 수 있는 것이 바람직하다.

또한, 상기 이용자는 프로그램 관리 정보 설정을 통하여 유해 차단 여부 설정, 유해 사이트 접속시 디스플레이 설정, 원격 관리 여부 설정, 암호 변경 설정 및 프로그램 숨기기 기능 설정 중 선택된 어느 하나 이상의 정보를 설정하여, 상기 설정된 정보를 실행시킬 수 있는 것이 바람직하다.

또한, 상기 이용자는 프로그램 사용 제한 설정을 통하여 상기 이용자가 지정한 하나 이상의 프로그램에 대한 사용을 차단할 수 있는 것이 바람직하다.

여기서, 상기 이용자는 프로그램 제한 시간 설정을 통하여 상기 이용자가 지정한 시간에 이용자가 지정한 프로그램에 대한 사용을 차단할 수 있는 것이 바람직하다.

또한, 상기 이용자는 인터넷 사용 제한 정보 설정을 통하여 상기 이용자가 지정한 시간에 인터넷 사용을 차단할 수 있는 것이 바람직하다.

또한, 상기 이용자는 유해 주소 차단 정보 설정을 통하여, 이용자에 의해 지정된 문자가 포함되는 정보 제공자 주소를 차단할 수 있는 것이 바람직하다.

이와 더불어, 상기 사업자가 웹 상에 구축하는 데이터베이스에는 회원 정보 데이터베이스, 유해 정보 데이터베이스 및 관련 정보 데이터베이스 중 선택된 어느 하나 이상의 데이터베이스를 포함하여 구축하는 것이 바람직하다.

한편, 상기 제1항 내지 제11항 중 선택된 어느 한 항의 통신 네트워크를 이용한 정보 차단 서비스 사업 방법을 수행할 수 있는 프로그램이 수록된 컴퓨터로 읽을 수 있는 기록매체에 의해 본 발명의 목적이 달성될 수 있다.

상기와 같은 본 발명의 통신 네트워크를 이용한 정보 차단 서비스 사업 방법은 서버 컴퓨터로 읽을 수 있는 기록 매체에 저장될 수 있다. 이러한 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있도록 프로그램 및 데이터가 저장되는 모든 종류의 기록매체를 포함한다. 그 예로는, 롬(Read Only Memory), 램(Random Access Memory), CD(Compact Disk)-Rom, DVD(Digital Video Disk)-Rom, 자기 테이프, 플로피 디스크, 광데이터 저장장치등이 있으며, 또한 케리어 웨이브(예를 들면, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함된다. 또한, 이러한 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

이하, 본 발명을 구체적으로 설명하기 위해 실시예를 들어 설명하고, 발명에 대한 이해를 돕기 위해 첨부 도면을 참조하여 상세하게 설명하기로 한다. 그러나, 본 발명에 따른 실시예들은 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 아래에서 상술하는 실시예들에 한정되는 것으로 해석되어지지 않아야 한다. 본 발명의 실시예들은 당업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되어지는 것이다.

도 1은 본 발명에 따른 네트워크를 이용한 유해 정보 차단 서비스 사업 방법의 일실시예를 설명하기 위한 네트워크 구성도이다.

상기 도 1에 도시된 바에 따르면, 유해 정보 차단 서비스 사업자(10)는 회원 정보 데이터베이스(13), 유해 정보 데이터베이스(14) 및 관련 정보 데이터베이스(15)와 상기 데이터베이스들(13, 14, 15)과 연동되는 다수개의 서버들(12)과 유해 정보 검색 로봇(11)을 구비하고 인터넷(40)을 통하여 소정 사이트/홈 페이지 및 유해 정보 차단 프로그램을 이용자(30)의 컴퓨터에 탑재한 이용자(30) 컴퓨터와의 접속이 이루어져 있다.

여기서, 상기 사업자(10)는 이용자(30)에게 유해 정보 차단 서비스를 제공하기 위하여, 사업자(10)가 유해 정보 검색 로봇(11)을 이용하여 수집한 유해 정보를 상기 사업자(10)의 서버(12)에 연동되는 유해 정보 데이터베이스(14)에 구축하거나, 이용자(30)가 온/오프 라인을 통해 제공한 유해 정보를 상기 서버(12)에 연동되는 유해 정보 데이터베이스(14)에 구축한다.

이때, 상기 이용자(30)는 이용자(30)의 컴퓨터에 탑재된 유해 정보 차단 프로그램을 구동하여 소정 사이트 또는 홈 페이지 방문시, 상기 프로그램에 의한 1차 유해 검색 체크를 하며, 상기 검색 체크를 통과한 경우 이용자(30)가 사업자(10)의 유해 정보 데이터베이스(14)에 의뢰하는 2차 유해 검색 체크를 수행한다.

여기서, 상기 소정 사이트 또는 홈 페이지의 URL은 윈속 2를 통하여 서버(12)에 의뢰되고, 상기 서버(12)는 이용자(30)의 요청에 의해 유해 정보 데이터베이스(14)를 검색하여 유해 정보 여부를 이용자(30)에게 전달하며, 상기 서버(12)에 의뢰한 결과 값이 유해 사이트일 경우 이용자(30)의 웹 브라우저에 리다이렉트(redirect)된 URL 메시지를 전달함으로서 웹 사이트 접근을 차단한다.

또한, 상기 유해 정보 검색 로봇(11)은 서버와 연동하여 1대 이상의 컴퓨터에서 작동이 가능하며, 특정 IP 주소의 유해 사이트 검색 및 특정 사이트로 부터의 링크를 통해 유해 사이트를 추적한다. 즉, 유해 사이트의 추적에 대한 일련의 작업이 검색 로봇에 의해 자동으로 가동되어 유해 사이트를 파악하고, 상기 유해 사이트의 주소를 유해 정보 데이터베이스(14)에 자동으로 입력한다.

이때, 상기 유해 정보 검색 로봇(11)은 유해 정보 사이트의 링크 사이트를 추적해 나가는 방식을 통하여 유해 정보 사이트에 대한 데이터를 구축한다. 즉, 소정 유해 사이트의 주소가 주어지면 유해 사이트의 웹 페이지의 내용을 텍스트로 변환하여 어구 분석 작업을 통해 유해 사이트에 포함된 본문의 내용과 링크된 URL 주소만을 데이터베이스에 기록하게 되며, 어구 분석된 본문의 내용을 검색하여 유해 정보 사이트 판단시 자동으로 데이터베이스에 입력이 이루어진다.

또한, 상기 유해 정보 검색 로봇(11)은 상기 링크된 URL의 어구 분석 작업을 통하여 반복된 작업을 거쳐 유해 사이트에 링크된 사이트에 대한 추적 작업 및 데이터베이스 입력 작업이 이루어지며, 소정 IP 주소를 기반으로 IP 주소 및 포트 검색을 통한 웹 서비스 검색을 통해 순차적으로 IP 주소의 웹 사이트 내용을 검색한다.

이와 더불어, 상기 유해 정보 검색 로봇(11)은 신규 사이트 및 일반 포털 사이트의 변경 사항을 수시로 체크하여 최신의 검색 데이터를 유지함은 당업자에게 있어서 자명하다.

또한, NMS(Network Management Service, 네트워크 관리 시스템) 엔진을 탑재시켜 연결되지 않는 사이트등의 관리는 전용 NMS 엔진과 검색 로봇(11)이 주기적으로 검사하고, 일정 사이트내의 라우터(router) 또는 ISP(Instruction Set Processor, 명령어 집단 처리기)등을 동시에 데이터베이스화 한 후 NMS 엔진의 검색 결과 ISP자체의 다운등 회선 불량과 더불어 결점 검사 로봇의 주기적 검사를 한다.

여기서, 상기 서버(12)는 복수대가 구비되어 이용자(30)가 상기 서버(12)에 유해 정보를 의뢰하면, 복수대의 서버에 분산 의뢰하여 네트웍 트래픽 및 서버의 과부하를 방지한다. 즉, 상기 이용자(30)가 사업자(10)의 서버(12)로 유해 정보를 요구할 때, 이용자(30) 컴퓨터의 하드 디스크 시리얼(serial)을 기반으로 랜덤 키(random key)를 생성시켜 생성된 키에 따라 각각 다른 서버에 요청한다.

한편, 상기 네트워크의 구성 주체로 사업을 보조하거나 별도의 전문적인 서비스를 제공할 수 있는 관련업체 서비스업자가 더 포함되어 인터넷(40)에 접속될 수 있으며, 상기 사업자(10)의 서버(12)에 연동되는 데이터베이스로 관련업체 서비스 데이터베이스가 더 구축될 수 있다.

도 2는 본 발명에 따른 서비스 사업 방법의 유해 정보 차단 프로그램의 동작을 설명하기 위한 블럭도이다.

상기 유해 정보 차단 프로그램의 동작은 SQL(Structured Query Language, 구조화질의 언어) 서버(80), 유해 사이트 판단 서버(70), 유해 사이트 판단 모듈(60) 및 차단 엔진(50)의 연동 동작으로 이루어진다.

상기 유해 정보 차단 프로그램의 동작 방식은 인터넷 이용자가 접근하고자 하는 사이트의 URL을 차단 엔진(50)이 추출하면 상기 사이트에 접근을 시도하기 전에 블로킹 콜(blocking call)을 통해 동작을 잠시 정지시킨 후 추출된 URL을 유해 사이트 판단 모듈(60)에 전달한다.

이어서, 상기 유해 사이트 판단 모듈(60)은 차단 엔진(50)으로부터 전송받은 URL을 유해 사이트 판단 서버(70)에 전송한다. 이때, 유해 사이트 판단 모듈(60)도 윈속(winsock)을 통과하게 되므로 다시 유해 사이트 판단 모듈을 거치는 반복 현상(recursion)이 발생하지 않도록 차단 엔진(50)에서 유해 사이트 판단 서버(70)를 거치는 요구 사항은 처리를 하지 않도록 한다.

이어서, 상기 유해 사이트 판단 서버(70)는 ISAPI(Information Separator Application Program Interface, 국제 표준 응용 프로그램 인터페이스)를 통해 SQL 서버(80)에 상기 URL을 전달하여 유해 사이트 여부를 판단한다.

이때, 상기 URL에 해당되는 사이트가 유해 사이트라면 유해 사이트 판단 모듈(60)은 차단 엔진(50)에 유해 사이트임을 알리고 윈속 2에 의해 캡슐화된 커넥트를 통해 상기 URL 사이트로의 접속 차체를 차단한다. 즉, 이용자가 유해 사이트로 접근을 시도하면 실제 HTTP 리퀘스트가 목적 사이트에 도착하기 전에 상기 URL에 해당하는 유해 사이트의 유해 여부가 파악되어 차단된다.

여기서, 상기 동작 방식은 정보 제공자 사이트에 접근이 이루어지고 데이터를 전송받은 후 전송받은 데이터를 기준으로 차단함으로서 불필요한 데이터를 다운로드받아 네트워크 속도가 저하되고 유해 사이트의 내용이 이용자에게 일정 부분 보여진 후 차단되는 동작의 불안정성등을 방지한다.

또한, 이용자의 모든 HTTP 리퀘스트가 서버(70, 80)를 통해 확인 절차를 거치기 때문에 상기 서버(70, 80)에서 이용자의 인터넷 사용 내역을 효과적으로 관리할 수 있음은 당업자에게 자명하다.

이와 더불어, 상기 유해 사이트 판단 모듈(60)과 유해 사이트 판단 서버간에 주고받는 데이터는 하나의 HTTP 리퀘스트에 대하여 최대 110바이트이므로, 서버의 부담을 최소화할 수 있고, 상기 차단 엔진(50)은 이용자의 HTTP 리퀘스트를 분석하여 소정 사이트에 대해 평균 1회의 유해 사이트 판단만을 한다.

여기서, 윈속 2 기반의 차단 엔진(50)은 네트워크 응용 프로그램들의 동작과 상기 응용 프로그램들이 사용하는 네트워크 함수들을 모니터링하여 모니터링 및 차단에 대한 함수를 실행시킨다.

도 3은 본 발명에 따른 서비스 사업 방법의 이용자가 사업자의 서버에 접속하여 필요한 서비스 정보를 선택하는 과정의 일실시예를 나타내는 흐름도이다.

상기 도 3에 도시된 바와 같이, 상기 이용자는 필요한 서비스 정보를 사업자로 부터 제공받기 위하여 사업자의 인터넷을 통해 사업자의 홈 페이지에 접속하는 단계(S11)를 수행한다. 이어서, 상기 이용자는 사업자가 제공하는 유해 정보 차단 프로그램을 설치할 것인가를 판단(S12)한다.

이때, 상기 이용자가 이용자의 컴퓨터에 상기 프로그램을 설치하지 않았으면 상기 프로그램을 설치하는 단계(S13)를 실행하고, 상기 프로그램이 설치되어 있으면 사업자의 홈 페이지에서 제공하는 서비스 정보를 선택하는 단계(S14)를 실행한다.

여기서, 상기 이용자는 별도의 회원 로그인이나 보안 인증의 수행 유무에 상관없이 상기 프로그램을 다운로드 받을 수 있으며, 차

후에 사업자의 필요에 따라 상기 회원 로그인이나 보안 인증의 절차를 수행한 이용자에게만 서비스를 제공할 수 있음은 자명하다.

또한, 상기 단계(S13)의 프로그램 설치는 사업자가 제공하는 상기 프로그램을 다운로드 받아 이용자의 컴퓨터에 탑재하거나, 오프라인 상으로 사업자에 의해 제공된 상기 프로그램이 수록된 기록매체를 구동시켜 프로그램을 설치할 수 있음은 자명하다.

여기서, 상기 사업자가 제공하는 서비스 정보는 원격 관리 정보, 회원 정보 변경, 로그인 정보 분실, 묻고 답하기 및 관련 정보등에 대한 서비스 정보를 제공한다.

이어서, 상기 단계(S13) 이후에 상기 사업자는 이용자가 회원 로그인 정보를 입력했는지 여부를 판단하여 상기 이용자가 회원 로그인 정보를 정확하게 입력하면 상기 이용자가 선택한 정보를 디스플레이하는 단계(S17)를 실행하고, 상기 이용자가 회원 로그인 정보를 입력하지 않았거나 정확한 회원 로그인 정보를 입력하지 않았으면, 사업자는 회원 정보 및 유해 차단 서비스 이용에 관한 정보를 요구하여 회원 등록(S16)시킨다. 이어서, 상기 등록된 회원 정보는 서비스 사업자의 웹 서버에 연동되는 회원 정보 데이터베이스에 저장하고, 서비스 사업자는 이용자에게 서비스 정보 선택 페이지를 디스플레이한다.

이어서, 단계(S17) 이후에 사업자는 이용자가 다른 정보의 선택 여부를 판단하여 이용자가 다른 정보를 선택하면 서비스 정보 선택 페이지를 디스플레이(S19)한다.

도 4는 본 발명에 따른 서비스 사업 방법의 사업자가 이용자에게 제공하는 원격 관리 리스트 웹 페이지의 일실시예이다.

상기 도 4에 도시된 바와 같이, 이용자가 상기 도 3에서와 같이 사업자가 제공하는 서비스 정보 중 원격 관리 정보를 선택하고 로그인 정보를 입력하면, 사업자는 이용자에게 원격 관리 리스트가 포함된 웹 페이지를 디스플레이한다.

상기 원격 관리 리스트는 이용자가 최초 설정한 유해 사이트 정보 또는 사업자가 구축한 유해 정보를 기초로 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 유해 사이트를 방문하면 자동으로 사업자의 서버에 연동되는 회원 정보 데이터베이스로 유해 사이트 접속 시간(110) 및 유해 사이트 URL 주소(120)가 저장되어, 상기 이용자가 인터넷 접속이 가능한 장소에서 사업자의 홈페이지에 접속하여 이용자 컴퓨터의 유해 차단 기록을 볼 수 있다.

여기서, 상기 이용자는 원격 관리 리스트를 통하여 사업자에 의해 원격 관리로 보관되어 있는 텍스트 문서나 엑셀, 스프레드 시트로 저장이 가능함은 당업자에게 있어 자명하다.

도 5는 본 발명에 따른 서비스 사업 방법에서 유해 차단 프로그램 실행 과정의 일실시예를 나타내는 흐름도이다.

상기 도 5에 도시된 바와 같이, 상기 유해 차단 프로그램의 실행 과정은 이용자가 로그인 정보 또는 보안 인증 정보를 입력(S21)하면 상기 프로그램은 상기 정보가 정확한지를 판단(S22)하여 이용 정보 선택창을 디스플레이(S24)시킨다.

이때, 상기 이용자가 정확한 정보를 입력하지 않았다면 단계(S21)로 리턴하여 상기 정보를 재입력(S23)한다.

여기서, 상기 이용 정보 선택창은 기록 보기 아이콘, 일반 설정 아이콘, 프로그램 사용제한 아이콘, 프로그램 제한시간 아이콘, 인터넷 사용제한 아이콘 및 개별 차단 아이콘등을 포함하여 구성된다.

이어서, 상기 단계(S24) 이후에 이용자는 상기 이용 정보 선택창의 아이콘들중 하나를 선택하여 이용 정보를 실행(S25)한다.

이어서, 상기 단계(S25) 이후에 이용자는 다른 정보를 선택할 것인가를 판단하여 다른 정보를 선택한다면 단계(S24)로 리턴(S27)하고, 다른 정보를 선택하지 않는다면 프로그램을 종료(S28)한다.

도 6은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 이용 정보 중 기록 보기를 선택하는 과정의 일실시예를 나타낸 흐름도이다.

상기 도 6에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 이용 정보 중 기록 보기를 선택하는 과정은 이용자가 상기 도 5의 이용 정보 선택창을 디스플레이시키는 단계(S24) 이후에 기록 보기 아이콘을 선택하여 기록 보기창을 디스플레이(S31)시킨다.

이때, 상기 기록 보기창은 인터넷 사이트 차단 기록 보기 아이콘, 인터넷 사용 기록 보기 아이콘 및 날짜별 인터넷 사용 기록 보기 아이콘등을 포함하여 구성된다.

이어서, 상기 단계(S31) 이후에 이용자는 상기 차단 기록 보기 아이콘들중 하나를 선택하여 차단 기록 보기를 실행(S32)한다.

이어서, 상기 단계(S32) 이후에 이용자는 다른 정보를 선택할 것인가를 판단하여 다른 정보를 선택한다면 단계(S31) 또는 도 5의 단계(S24)로 리턴(S34)하고, 다른 정보를 선택하지 않는다면 프로그램을 종료(S35)한다.

도 7은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 인터넷 차단 기록 보기창의 일실시예이다.

상기 도 7에 도시된 바와 같이, 상기 인터넷 차단 기록 보기창은 이용자가 최초 설정한 유해 사이트 정보 또는 사업자가 구축한 유해 정보를 기초로 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 유해 사이트를 방문한 정보를 데이터 시트 또는 일반 문서로 제공한다.

여기서, 상기 인터넷 차단 기록 보기창은 상기 사용자가 유해 사이트를 방문한 기록을 로그 구분(210), 유해 사이트 접속 시간(220) 및 유해 사이트 URL 주소(230)별로 세분화하여 제공하며, 이용자에 의해 상기 인터넷 차단 기록의 저장, 삭제 및 인쇄가 가능하다.

또한, 상기 차단 기록 보기는 원격 관리가 가능하게 설계되어 있으며 인터넷이 연결되어 있어야 사용이 가능하고, 인터넷 사용 기록과 쿠키 기록은 웹 브라우저의 캐시 화일을 관리한다.

도 8은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 인터넷 사용 기록 보기창의 일실시예이다.

상기 도 8에 도시된 바와 같이, 상기 인터넷 사용 기록 보기창은 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 인터넷에 접속 후 방문한 모든 웹 사이트의 주소를 디스플레이하며, 이용자가 웹 사이트들의 목록 중 어느 하나(320)를 선택하여 해당 사이트를 디스플레이시킬 수 있고, 상기 해당 사이트의 최신 정보인 최근 접근 시간, 최근 검사 시간, 최근 수정 시간, 만기일, 방문수 및 URL 주소등을 볼 수 있다.

도 9는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 일반 설정을 하는 과정의 일실시예이다.

상기 도 9에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 이용 정보 중 상기 프로그램의 일반 설정을 하는 과정은 이용자가 상기 도 5의 이용 정보 선택창을 디스플레이시키는 단계(S24) 이후에 일반 설정 아이콘을 선택하여 일반 설정창을 디스플레이(S41)시킨다.

이때, 상기 일반 설정창은 유해 차단 여부 설정 아이콘, 유해 사이트 접속시 설정 아이콘, 원격 관리 여부 설정 아이콘, 암호 변경 설정 아이콘 및 프로그램 숨기기 기능 설정 아이콘등을 포함하여 구성된다.

여기서, 상기 이용자는 유해 차단 여부 설정을 통하여 이용자가 유해 차단을 할 것인지에 대한 여부를 설정하며, 상기 유해 사이트 접속시 설정을 통하여 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 인터넷에 접속 후 유해 사이트를 방문시, 상기 프로그램에 의해 유용한 사이트 디스플레이, 유해 사이트 로그 표시창 디스플레이, 연결되지 않는 사이트 표시창 디스플레이, 검색엔진 디스플레이 및 빈 페이지 디스플레이 중 선택된 어느 하나의 사이트 및 표시창의 선택 여부를 설정하며, 상기 원격 관리 여부 설정을 통하여 이용자가 사업자의 홈 페이지에 접속하여 원격 관리를 할 것인지에 대한 선택 여부를 설정하며, 상기 암호 변경 설정을 통하여 암호 변경을 할 것인지에 대한 선택 여부를 설정하며, 상기 프로그램 숨기기 기능 설정을 통하여 작업 표시줄에 프로그램의 아이콘을 표시할 것인지에 대한 여부를 설정한다.

이어서, 상기 단계(S41) 이후에 이용자는 상기 일반 설정 아이콘들 중 어느 하나를 선택하여 설정한 후, 상기 설정된 정보를 확인(S42)한다.

도 10은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 프로그램 사용 제한창의 일실시예이다.

상기 도 10에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 이용 정보 중 상기 프로그램의 프로그램 사용 제한 설정을 하는 과정은 이용자가 상기 도 5의 이용 정보 선택창을 디스플레이시키는 단계(S24) 이후에 프로그램 사용 제한 아이콘을 선택하여 프로그램 사용 제한창을 디스플레이시킨다. 이어서, 상기 이용자는 오락, 증권 및 특정 프로그램등의 사용자 프로그램을 추가 또는 삭제할 것인지를 판단(S51)하여 사용자 프로그램을 추가한다면, 제한할 프로그램을 지정하여 제한 프로그램 리스트에 추가(S52)시킨다.

이어서, 상기 단계(S52) 이후에 상기 이용자는 더 추가할 사용자 프로그램이 있는지를 판단하여 만약 더 추가할 사용자 프로그램이 있으면 단계(S52)로 리턴(S54)하고, 만약 더 추가할 프로그램이 없으면 설정된 정보를 확인(S55)한 후, 프로그램 사용 제한 설정 과정을 종료한다.

한편, 상기 단계(S51) 이후에 이용자가 제한한 프로그램들 중 프로그램 사용 제한을 해제하고자 한다면 제한 프로그램 리스트에 포함된 사용자 프로그램들 중 어느 하나를 선택하여 삭제(S56)시킨다.

이어서, 상기 단계(S56) 이후에 상기 이용자는 더 삭제할 사용자 프로그램이 있는지를 판단(S57)하여 만약 더 삭제할 사용자 프로그램이 있으면 단계(S56)로 리턴(S58)하고, 만약 더 삭제할 프로그램이 없으면 설정된 정보를 확인(S55)한 후, 프로그램 사용 제한 설정 과정을 종료한다.

여기서, 상기 이용자가 프로그램 사용 제한 설정을 통하여 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 사용자 프로그램을 실행하는 것을 차단할 수 있다.

도 11은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 프로그램 시간 제한창의 일실시예이다.

상기 도 11에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 이용 정보 중 상기 프로그램의 프로그램 시간 제한 설정은 이용자가 상기 도 5의 이용 정보 선택창을 디스플레이시키는 단계(S24) 이후에 프로그램 사용 제한 아이콘을 선택하여 프로그램 시간 제한창을 디스플레이시킨다.

이때, 상기 프로그램 시간 제한창은 프로그램 제한 시간 아이콘(410) 및 인터넷 사용 제한 아이콘(420)등을 포함하여 구성된다.

여기서, 상기 이용자는 프로그램 시간 제한 또는 인터넷 사용 제한을 통하여 요일별 및 시간 단위별 프로그램의 사용 가능 및 금지를 설정할 수 있다.

도 12는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 개별 차단창의 일실시예이다.

상기 도 12에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 이용 정보 중 상기 프로그램의 개별 차단 설정은 이용자가 상기 도 5의 이용 정보 선택창을 디스플레이시키는 단계(S24) 이후에 개별 차단 아이콘을 선택하여 개별 차단창을 디스플레이시킨다.

이때, 상기 개별 차단창은 유해 단어 리스트(510), 유해 단어 입력창, 유해 단어 리스트에 유해 단어를 추가 또는 삭제할 수 있는 추가 및 삭제 아이콘, 유해 주소 리스트(520), 유해 주소 입력창 및 유해 주소 입력창에 유해 주소를 추가 또는 삭제할 수 있는 추가 및 삭제 아이콘을 포함하여 구성된다.

여기서, 이용자는 개별 차단을 통하여 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 유해 단어가 포함된 주소의 접속을 차단할 수 있다.

도 13은 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 설치, 업그레이드 및 삭제의 일실시예이다.

상기 도 13에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 설치, 업그레이드 및 삭제 과정은 유해 정보 차단 프로그램이 수록된 기록매체를 로딩(S61)하면 프로그램이 자동 설치(S62)된다.

이어서, 상기 단계(S62) 이후에 프로그램의 메인창이 디스플레이되고, 프로그램 이용자는 상기 메인창에 포함된 아이콘들중 어느 하나의 이용 정보를 선택(S63)한다.

여기서, 상기 메인창은 컴퓨터 검사하기 아이콘, 새로운 단어 목록 아이콘, 설치 및 업그레이드 아이콘, 추천 홈 페이지 아이콘 및 프로그램 삭제하기 아이콘등을 포함하여 구성된다.

이어서, 상기 단계(S63) 이후에 이용자는 상기 선택한 이용 정보를 실행시키고, 다른 이용 정보를 선택할 것인지를 판단(S65)한다.

이때, 상기 이용자가 다른 이용 정보를 선택하고자 한다면 단계(S63)으로 리턴(S66)하고, 다른 이용 정보를 선택하지 않는다면 프로그램을 종료(S67)한다.

여기서, 상기 이용자는 메인창의 이용 정보 중 어느 하나 이상의 정보를 실행함으로서, 이용자 컴퓨터의 하드 드라이브 내용 검색, 사업자의 서버와 연동하는 유해 정보 데이터베이스에 구축된 정보 검색, 상기 프로그램 업그레이드, 유익한 홈 페이지 검색 및 상기 프로그램 삭제등을 실행할 수 있다.

도 14는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 컴퓨터 검사창의 일실시예이다.

상기 도 14에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 메인창에 포함된 정보 중 상기 프로그램의 컴퓨터 검사하기 항목은 이용자가 상기 도 13의 메인창을 디스플레이시킨 이후에 컴퓨터 검사하기 아이콘을 선택하여 컴퓨터 검사하기창을 디스플레이시킨다.

이때, 상기 컴퓨터 검사하기창은 하드 디스크 선택(610), 검사 화일의 종류 선택(620), 검사 화일 리스트(630) 및 선택 화일 미리보기(640) 항목등을 포함하여 구성된다.

여기서, 상기 이용자는 상기 컴퓨터 검사하기를 통하여 검사 화일의 종류에 따른 선택된 하드 디스크의 화일들을 검사하고, 상기

검사된 화일들 중 어느 하나의 화일을 미리 볼 수 있으므로, 상기 이용자는 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 저장한 화일의 유해 여부를 확인할 수 있다.

도 15는 본 발명에 따른 서비스 사업 방법에서 유해 정보 차단 프로그램의 새로운 단어 목록창의 일실시예이다.

상기 도 15에 도시된 바와 같이, 상기 유해 정보 차단 프로그램의 메인창에 포함된 정보 중 상기 프로그램의 새로운 단어 목록 항목은 이용자가 상기 도 13의 메인창을 디스플레이시킨 이후에 새로운 단어 목록 아이콘을 선택하여 새로운 단어 목록창을 디스플레이시킨다.

이때, 상기 새로운 단어 목록창은 유해 단어 리스트(710) 및 이용자 컴퓨터에 설정된 유해 단어 목록 리스트(720)등을 포함하여 구성된다.

여기서, 상기 이용자는 상기 유해 단어 리스트(710)에 포함된 유해 단어들 중 하나 이상을 선택하여 이용자 컴퓨터의 유해 단어 목록에 포함시킬 수 있으며, 상기 이용자 컴퓨터에 유해 단어 목록을 설정함으로서, 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 인터넷 이용시에 상기 유해 단어 목록에 포함된 단어 검색 및 상기 단어가 포함된 유해 사이트의 접속을 차단할 수 있다.

도 16 내지 도 18은 본 발명에 따른 서비스 사업자가 서버에 구축한 데이터베이스 구축도들이다.

상기 도 16에 도시된 바와 같이, 상기 회원 정보 데이터베이스(13)는 신규, 갱신, 추가 및 삭제가 가능하며 이용자 신상 정보 데이터필드(13a) 및 원격 관리 정보 데이터필드(13b)들로 구성된다.

상기 이용자 신상 정보 데이터필드(13a)는 ID, 비밀번호, 성명, 암호 인증 정보, 주민 등록 번호, 연락처, 소속 단체, 주거 현황, 가족 사항, 직장 주소등의 정보들로 구성되어 있고, 상기 원격 관리 정보 데이터필드(13b)는 이용자 컴퓨터를 이용한 사용자가 유해 사이트에 접속한 유해 사이트 접속 일자 및 유해 사이트 주소 등의 정보들로 구성된다.

상기 도 17에 도시된 바와 같이, 상기 유해 정보 데이터베이스(14)는 신규, 갱신, 추가 및 삭제가 가능하며 유해 단어 정보 데이터필드(62a) 및 유해 사이트 정보 데이터필드(62b)들로 구성된다.

여기서, 상기 유해 단어 정보 데이터필드(62a) 및 유해 사이트 정보 데이터필드(62b)는 유해 정보 검색 로봇에 의해 실시간으로 최신 유해 정보가 구축된다.

상기 도 18에 도시된 바와 같이, 상기 관련 정보 데이터베이스(15)는 신규, 갱신, 추가 및 삭제가 가능하며 추천 사이트 정보 데이터필드(15a), 관련 업체 정보 데이터필드(15b), 불편 접수 정보 데이터필드(15c), 프로그램 이용 정보 데이터필드(15d), 뉴스 정보 데이터필드(15e) 및 광고 정보 데이터필드(15f)들로 구성된다.

상기에서 설명한 본 발명에 따른 유해 정보 차단 프로그램은 차단 기록 보기를 통하여 유해 정보 차단 프로그램이 접속을 허락하지 않는 사이트에 대한 기록을 조회, 저장 및 삭제할 수 있으며, 날짜별 인터넷 사용 기록 보기를 통하여 이용자 컴퓨터의 사용자가 인터넷을 사용했던 기록들을 볼 수 있으며, 이용자가 상기 프로그램이 제공하는 다양한 설정을 통해 유해 정보에 대한 유입을 원천적으로 차단할 수 있다.

또한, 인터넷 사용 시간 제한을 통하여 인터넷의 특정 시간 및 요일별 사용 제한이 가능하고, 프로그램 사용 제한을 통하여 오락, 증권 및 특정 프로그램의 시간대별 사용 제한이 가능하고, 특정 사이트 개별 관리를 통하여 특정 단어 차단 및 사이트별 통제가 가능하고, 원격 관리를 통하여 인터넷을 통한 원격지에서의 유해 정보 차단 로그를 검색할 수 있고, 상기 로그 화일의 내용을 출력할 수 있다.

이와 더불어, 서비스 사업자는 유해 사이트 검색 및 차단, 단어 검색 차단 및 유해 정보 데이터베이스 검색 차단 방식을 동시에 지원하여 유해 사이트 차단에 있어서 오차단율을 최소화하고, 유해 차단 검색 로봇을 이용하여 신규 음란 사이트에 대한 최신 정보를 실시간으로 유해 정보 데이터베이스에 구축함으로서 실시간 유해 정보 데이터베이스 업데이트를 시킬 수 있다.

여기서, 상기 서비스 사업자는 유해 정보 차단의 신속성과 유해 정보 사이트만을 차단시키는 정확성을 높이기 위하여 유해 정보 차단 프로그램 구동에 의한 이용자 컴퓨터의 1차 유해 정보 차단과 상기 사업자 서버와의 접속에 의한 2차 유해 정보 차단이 이루어진다.

이때, 상기 사업자는 상기 1차 및 2차 유해 정보 차단시, 유해 정보 차단 프로그램의 이용자 설정에 의한 제 1 및 2 검색 단계, 비검색 사이트 중 유익하다고 인정되는 공인 사이트(예를 들어, 정부 기관 사이트)를 검색하는 제 3 검색 단계, 검사된 유익한 사이트를 검색하는 제 4 검색 단계, 검사된 유해 사이트를 검색하는 제 5 검색 단계, 유해 단어가 포함된 사이트를 검색하는 제 6 검색 단계 및 사업자의 유해 정보 데이터베이스와 연동된 서버와의 접속에 의한 제 7 검색 단계의 검색 레벨을 부여한다.

여기서, 상기 유해 정보 차단 프로그램은 다양한 브라우저 지원과 상기 프로그램을 수록한 기록매체를 이용자 컴퓨터에 삽입시 자동으로 설치될 수 있음은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에게 당연하다.

또한, 상기 서비스 사업자와 이용자의 다양한 인터넷 커뮤니케이션을 통하여 학부모 감시단 구성, 청소년 유해 정보 차단 단원 구성등을 통해 프로그램 이용자의 실질적 참여에 따른 건전한 인터넷 문화를 형성할 수 있음은 자명하다.

전술한 본 발명에서는 회원제로 운영하면서, 일정한 회원비를 징수하거나, 제공되는 정보에 따라 차등화된 요금을 부과하며, 전문 서비스를 제공하면서 발생되는 수익도 본 발명에 따른 사업의 수익원으로 예상될 수 있다.

이상에서 설명된 본 발명의 최적 실시예들이 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위해 사용된 것이 아니다.

발명의 효과

본 발명에 따르면, 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 특정 사이트 접속시, 7단계의 검색 레벨을 부여한 이용자 컴퓨터의 1차 유해 정보 차단 및 상기 사업자 서버와의 접속에 의한 2차 유해 정보 차단을 통하여 유해 정보 차단의 신속성과 유해 정보 사이트만을 차단시키는 정확성을 향상시킬 수 있다.

또한, 해당 사이트의 URL과 홈 페이지 타이틀의 내용을 1차적으로 검색하여 유해 단어의 사용 여부를 검색하고 유해 정보 데이터베이스 서버에 의뢰하지 않고도 1차적인 차단기능을 발휘함으로서 서버의 과부하 방지와 차단의 신속성을 유지할 수 있고, 유해 정보 의뢰시 다수의 유해 정보 데이터베이스 서버에 분산 의뢰하여 네트웍 트래픽 및 서버의 과부하를 방지하고 유해 정보 차단이 분산 처리가 될 수 있도록 안정화된 서비스를 구현할 수 있다.

또한, 유해 정보 데이터베이스와 연동한 실시간 차단을 이용함으로서 목록 업데이트가 필요없고, 학습 사이트 및 유익한 사이트까지 차단시키는 오류를 방지함과 동시에 유해 정보의 실시간 검색이 가능하다.

이와 더불어, 인터넷의 열린 공간 속의 수 많은 유해 환경에서 나만의 차단 설정을 통해 유해 정보에 대한 유입을 원천적으로 차단하고, 차단뿐만이 아닌 인터넷 관리 기능을 제시한 이용자 프로그램 조정기능도 함께 제공함으로서 청소년등이 인터넷을 통해 음란, 마약, 폭력등 유해 사이트에 접속하는 것을 사전에 차단하고 유해 환경으로 부터 보호할 수 있으며 청소년의 성장 과정에 맞춰 정보의 폭을 넓혀 주는 기능으로 인터넷의 올바른 사용법을 제시할 수 있는 효과가 있다.

(57)청구의 범위

청구항1

통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법에 있어서,

(a)사업자가 유해 정보 검색 수단을 이용하여 유해 정보를 실시간으로 분석 및 수집하고, 상기 유해 정보를 웹 서버에 연동되는 유해 정보 데이터베이스로 구축하는 단계;

(b)상기 사업자의 서버에 이용자가 통신 네트워크를 이용하여 접속한 후, 상기 사업자가 요구하는 회원 정보 및 유해 정보 차단 서비스 이용에 관한 정보를 입력하면, 사업자는 이용자가 입력한 정보를 웹 서버에 연동되는 회원 정보 데이터베이스로 구축하는 단계;

(c)상기 사업자가 사업자의 서버에 접속한 이용자에게 유해 정보를 차단시킬 수 있는 유해 정보 차단 프로그램을 제공하면, 이용자는 유해 정보 차단 프로그램을 이용자의 PC에 탑재하는 단계;

(d)상기 이용자가 유해 정보 차단 프로그램을 구동시켜 상기 이용자 PC의 유해 정보 차단 및 원격 관리 여부를 설정하고, 유해 정보 차단 기능을 실행시키는 단계; 및

(e)상기 사업자는 사업자의 서버에 접속한 이용자에게 유해 정보 사용에 대한 원격 조회 정보, 회원 관리 정보 및 유해 차단 관련 정보를 제공하는 단계;를 포함하여 진행하는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항2

제1항에 있어서,

상기 (a)단계의 유해 정보 검색 수단은 유해 사이트의 웹 페이지 본문 내용을 텍스트 언어로 변환하여 어구 분석 작업을 통해 상기 본문 내용과 링크된 웹 주소를 분류하고, 상기 링크된 웹 주소만을 데이터베이스에 기록하는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항3

제2항에 있어서,

상기 유해 정보 검색 수단은 어구 분석된 본문 내용을 검색하여 유해 정보 사이트 판단시 자동으로 데이터베이스에 입력이 이루어지게 하는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항4

제1항에 있어서,

상기 (d)단계의 유해 정보 차단 기능을 실행시키는 단계는, (d1)이용자가 암호 인증 정보를 입력하는 단계; 및

(d2)이용자가 인터넷 사용 기록 보기 정보 설정, 프로그램 관리 정보 설정, 프로그램 사용 제한 정보 설정, 프로그램 제한 시간 정보 설정, 인터넷 사용 제한 정보 설정 및 유해 주소 차단 정보 설정 중 선택된 어느 하나 이상의 정보를 설정하는 단계;를 더 포함하여 진행하는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항5

제1항에 있어서,

상기 이용자는 인터넷 사용 기록 보기를 통하여 인터넷 사이트 차단 기록, 인터넷 사용 기록 및 날짜별 인터넷 사용 기록을 볼 수 있는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항6

제1항에 있어서,

상기 (d)단계의 원격 관리는 이용자가 최초 설정한 유해 사이트 정보 또는 사업자가 구축한 유해 정보를 기초로 유해 정보 차단 프로그램을 탑재한 이용자 컴퓨터의 사용자가 유해 사이트를 방문하면 자동으로 사업자의 서버에 연동되는 회원 정보 데이터베이스로 유해 사이트 접속 시간 및 유해 사이트 주소가 저장되어, 상기 이용자가 인터넷 접속이 가능한 장소에서 사업자의 서버에 접속하여 이용자 컴퓨터의 유해 차단 기록을 볼 수 있는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항7

제4항에 있어서,

상기 이용자는 프로그램 관리 정보 설정을 통하여 유해 차단 여부 설정, 유해 사이트 접속시 디스플레이 설정, 원격 관리 여부 설정, 암호 변경 설정 및 프로그램 숨기기 기능 설정 중 선택된 어느 하나 이상의 정보를 설정하여, 상기 설정된 정보를 실행시킬 수 있는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항8

제4항에 있어서,

상기 이용자는 프로그램 사용 제한 설정을 통하여 상기 이용자가 지정한 하나 이상의 프로그램에 대한 사용을 차단할 수 있는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항9

제4항에 있어서,

상기 이용자는 프로그램 제한 시간 설정을 통하여 상기 이용자가 지정한 시간에 이용자가 지정한 프로그램에 대한 사용을 차단할 수 있는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항10

제4항에 있어서,

상기 이용자는 인터넷 사용 제한 정보 설정을 통하여 상기 이용자가 지정한 시간에 인터넷 사용을 차단할 수 있는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항11

제4항에 있어서,

상기 이용자는 유해 주소 차단 정보 설정을 통하여, 이용자에 의해 지정된 문자가 포함되는 정보 제공자 주소를 차단할 수 있는 것을 특징으로 하는 통신 네트워크를 이용한 유해 정보 차단 서비스 사업 방법.

청구항12

제1항에 있어서,

상기 사업자가 웹 상에 구축하는 데이터베이스에는 회원 정보 데이터베이스, 유해 정보 데이터베이스 및 관련 정보 데이터베이스 중 선택된 어느 하나 이상의 데이터베이스를 포함하여 구축하는 것을 특징으로 하는 통신 네트워크를 이용한 정보 차단 서비스 사업 방법.

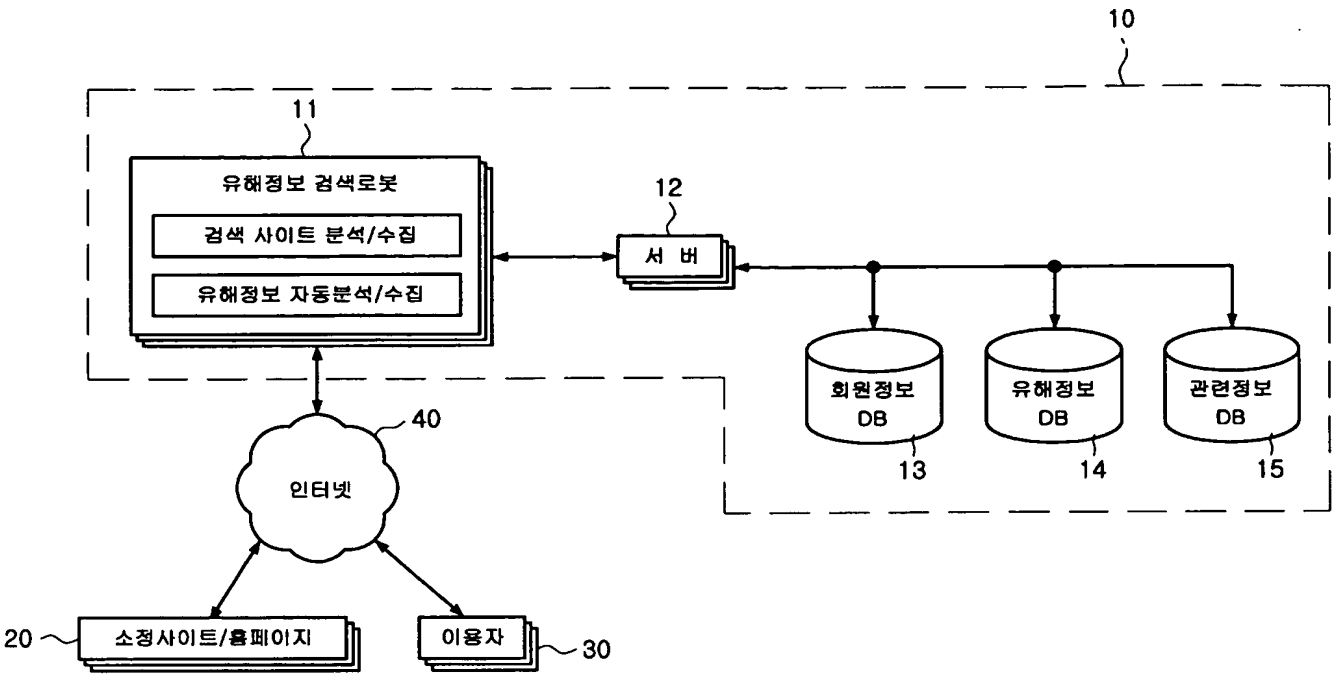
청구항13

상기 제1항 내지 제12항 중 선택된 어느 한 항의 통신 네트워크를 이용한 정보 차단 서비스 사업 방법을 수행할 수 있는 프로그램

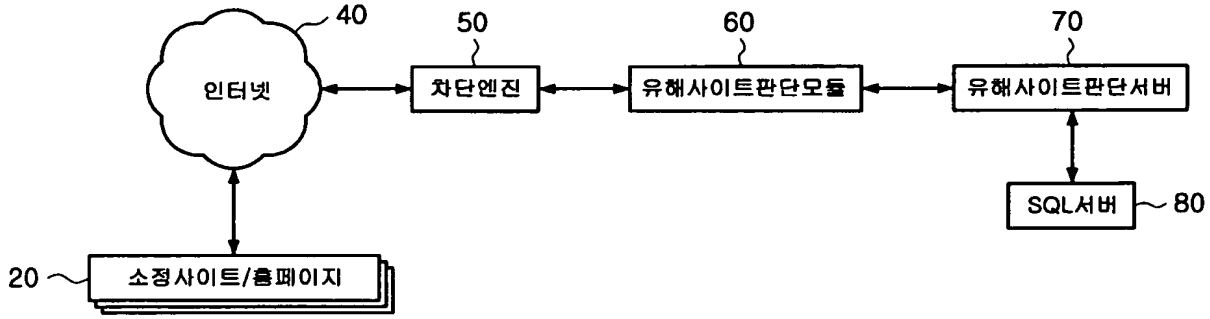
이 수록된 컴퓨터로 읽을 수 있는 기록매체.

도면

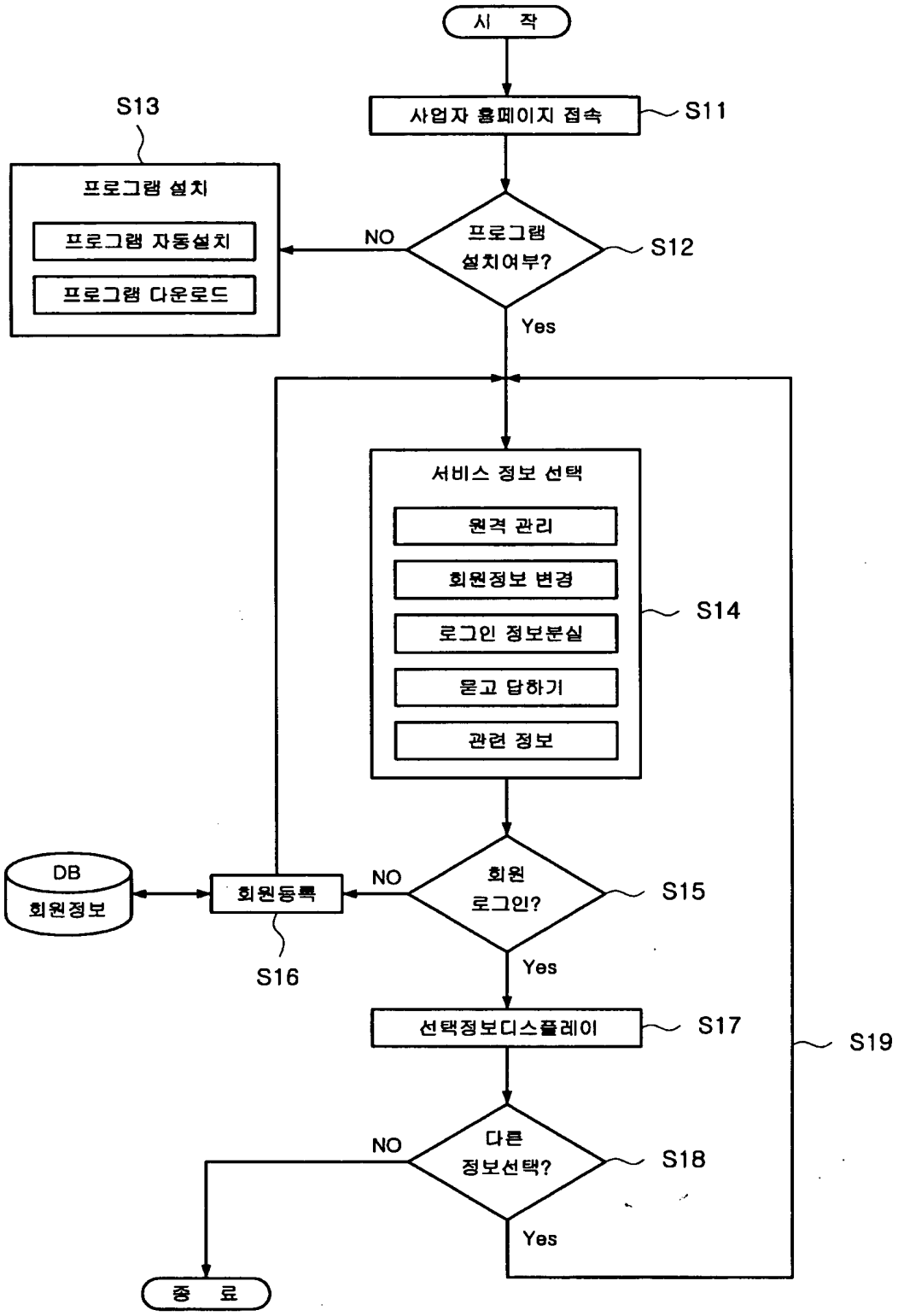
도면1



도면2



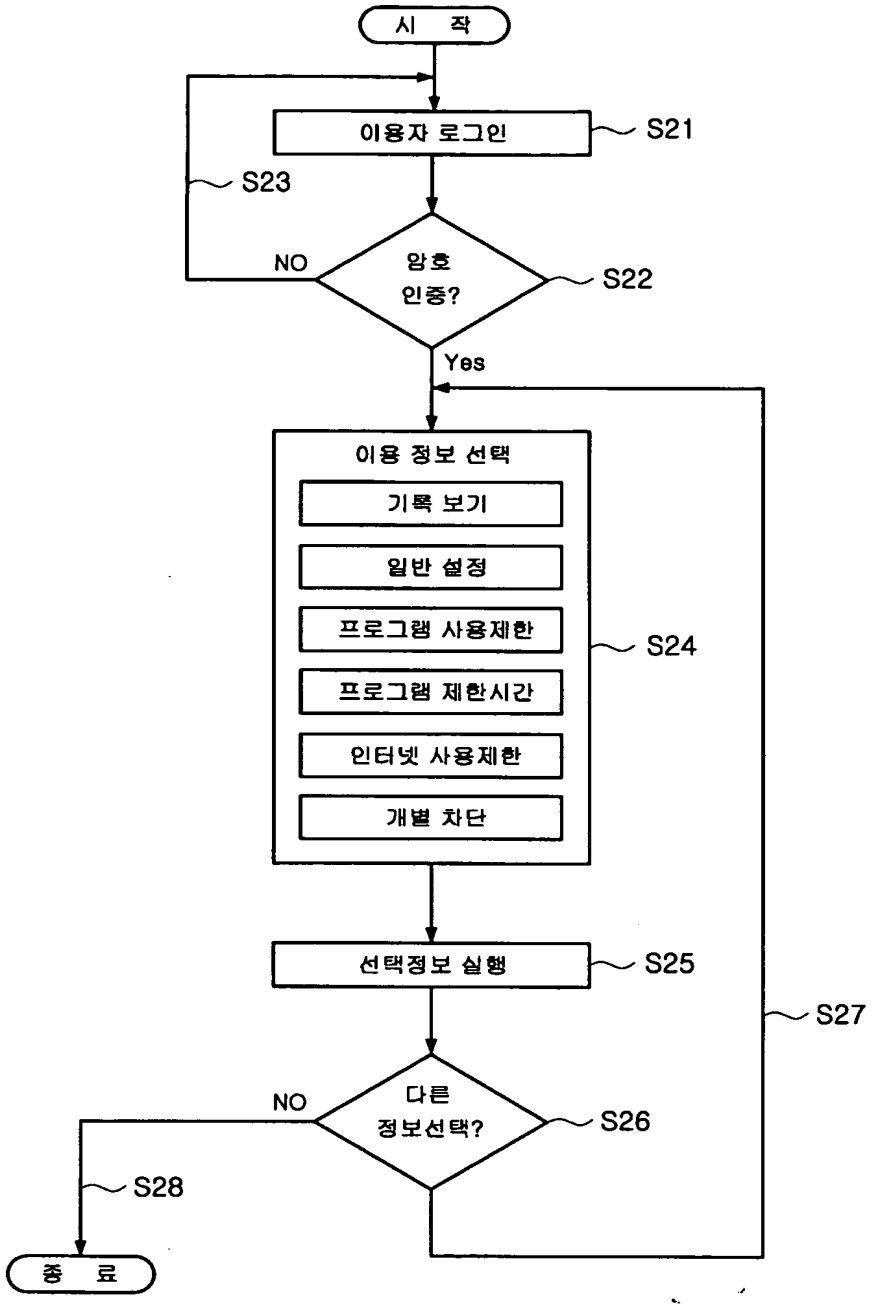
도면3


시 작
사업자 홈페이지 접속
S11
S13
프로그램 설치
프로그램 자동설치
프로그램 다운로드
NO
프로그램
설치여부?
S12
Yes
서비스 정보 선택
원격 관리
회원정보 변경
로그인 정보분실
묻고 답하기
관련 정보
S14
DB
회원정보
회원등록
NO
회원
로그인?
S15
S16
Yes
선택정보디스플레이
S17
S19
NO
다른
정보선택?
S18
Yes
종 료

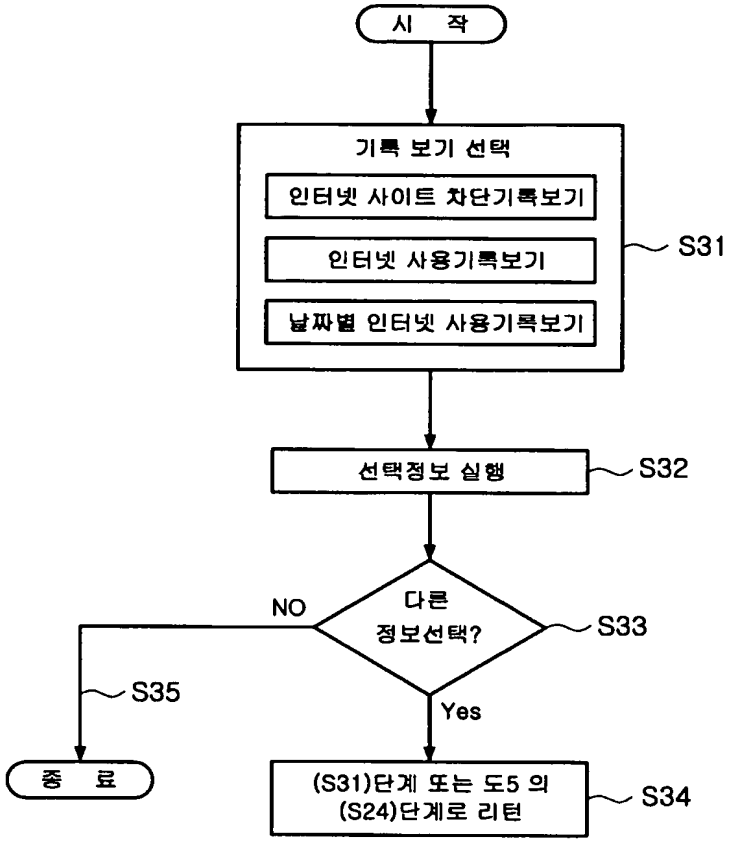
도면4


원격관리 리스트
pjy1017 님께서 설정하신 원격관리 현황입니다.
출 력
2000년 10월 04일 11:16
http://www.hangame.com/
2000년 10월 04일 11:15
http://www.hangame.com/popup/
2000년 10월 04일 11:14
http://www.hangame.com/
2000년 10월 04일 11:13
http://www.hangame.com/
2000년 10월 04일 11:13
http://www.hangame.com/
2000년 10월 04일 11:08
http://www.hangame.com/
2000년 10월 04일 11:08
http://www.hangame.com/popup/
2000년 10월 04일 11:06
http://www.yahoo.com/
2000년 10월 04일 11:06
http://www.yahoo.com/
이 전
다 음
총게시물1/1페이지
110
120

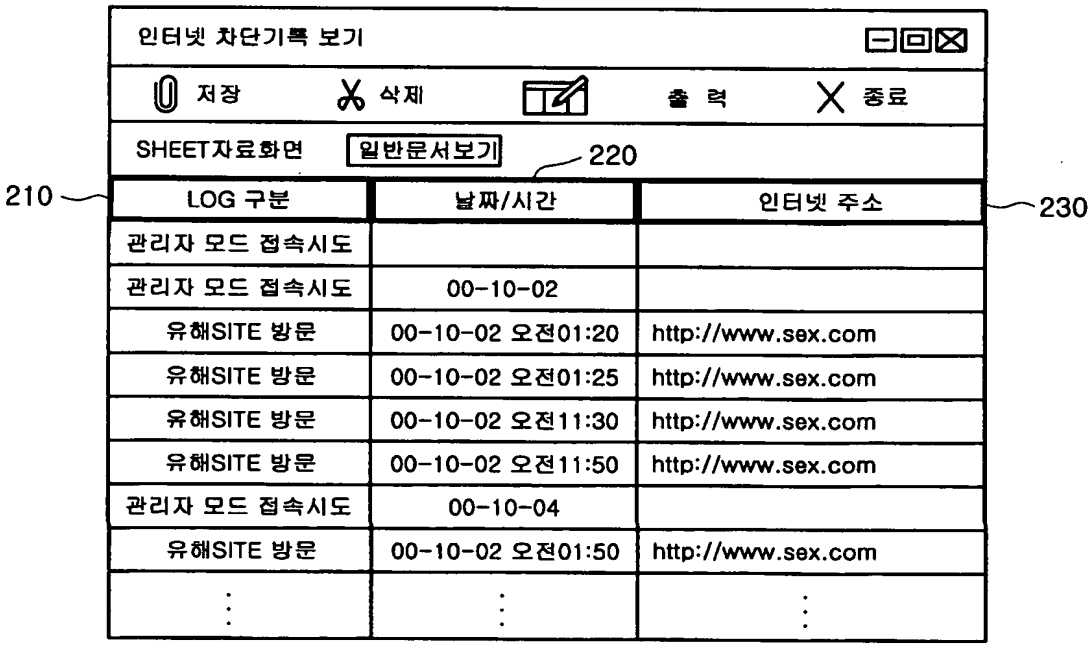
도면5


시 작
이용자 로그인
S21
S23
NO
암호
인증?
S22
Yes
이용 정보 선택
기록 보기
일반 설정
프로그램 사용제한
프로그램 제한시간
인터넷 사용제한
개별 차단
S24
선택정보 실행
S25
S27
NO
다른
정보선택?
S26
S28
종 료

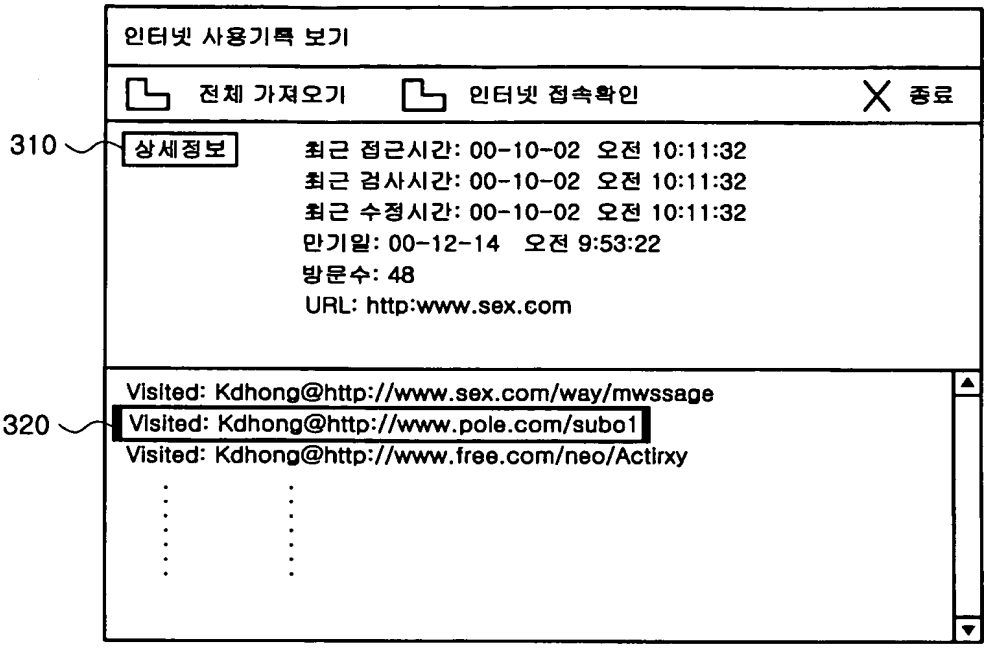
도면6


시 작
기록 보기 선택
인터넷 사이트 차단기록보기
인터넷 사용기록보기
날짜별 인터넷 사용기록보기
S31
선택정보 실행
S32
다른
정보선택?
S33
NO
Yes
S35
종 료
(S31)단계 또는 도5 의
(S24)단계로 리턴
S34

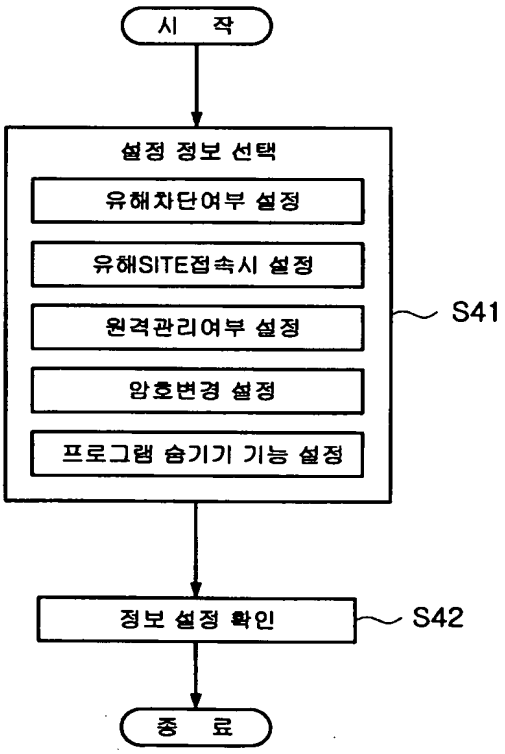
도면7


인터넷 차단기록 보기
저장
삭제
출 력
종료
SHEET자료화면
일반문서보기
220
210
LOG 구분
날짜/시간
인터넷 주소
230
관리자 모드 접속시도
관리자 모드 접속시도
00-10-02
유해SITE 방문
00-10-02 오전01:20
http://www.sex.com
유해SITE 방문
00-10-02 오전01:25
http://www.sex.com
유해SITE 방문
00-10-02 오전11:30
http://www.sex.com
유해SITE 방문
00-10-02 오전11:50
http://www.sex.com
관리자 모드 접속시도
00-10-04
유해SITE 방문
00-10-02 오전01:50
http://www.sex.com

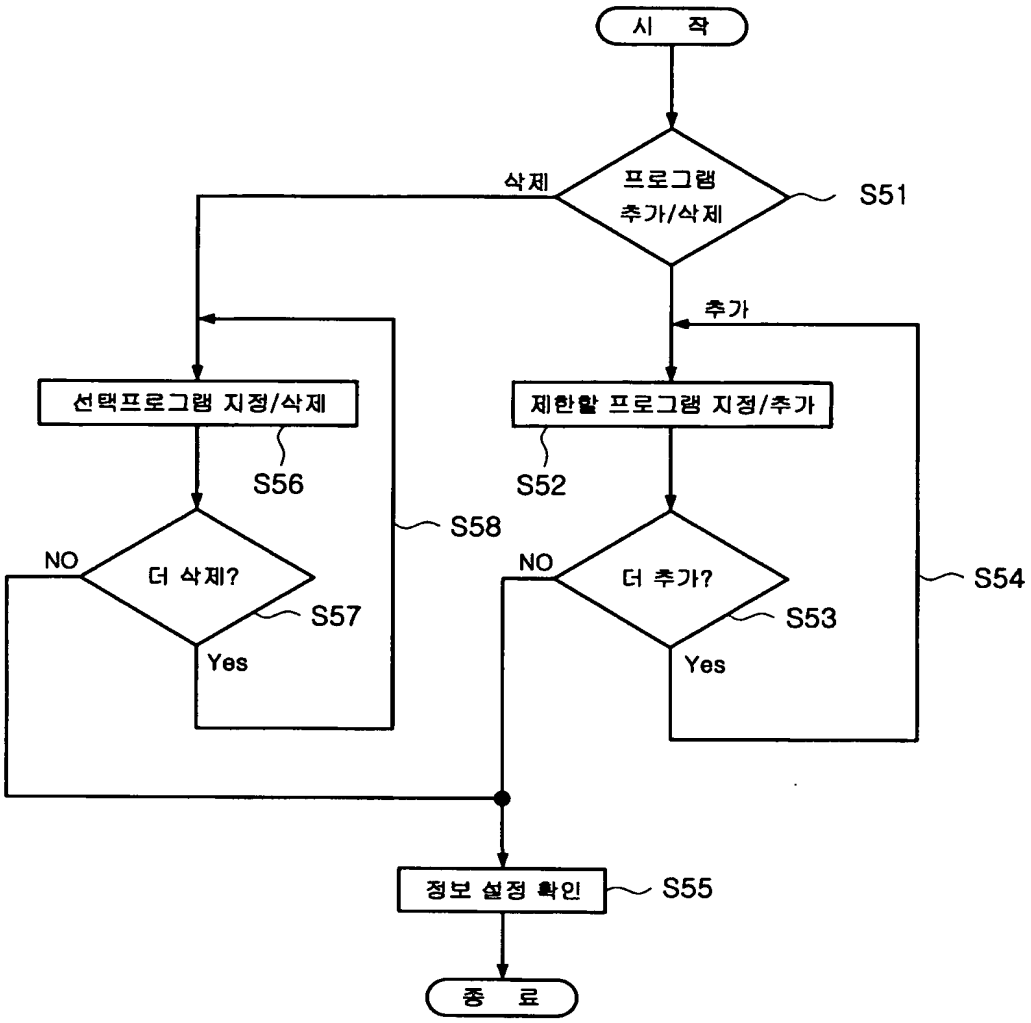
도면8


인터넷 사용기록 보기
전체 가져오기
인터넷 접속확인
종료
310
상세정보
최근 접근시간: 00-10-02 오전 10:11:32
최근 검사시간: 00-10-02 오전 10:11:32
최근 수정시간: 00-10-02 오전 10:11:32
만기일: 00-12-14 오전 9:53:22
방문수: 48
URL: http:www.sex.com
320
Visited: Kdhong@http://www.sex.com/way/mwssage
Visited: Kdhong@http://www.pole.com/subo1
Visited: Kdhong@http://www.free.com/neo/Actirxy

도면9


시 작
설정 정보 선택
유해차단여부 설정
유해SITE접속시 설정
원격관리여부 설정
암호변경 설정
프로그램 숨기기 기능 설정
S41
정보 설정 확인
S42
종 료

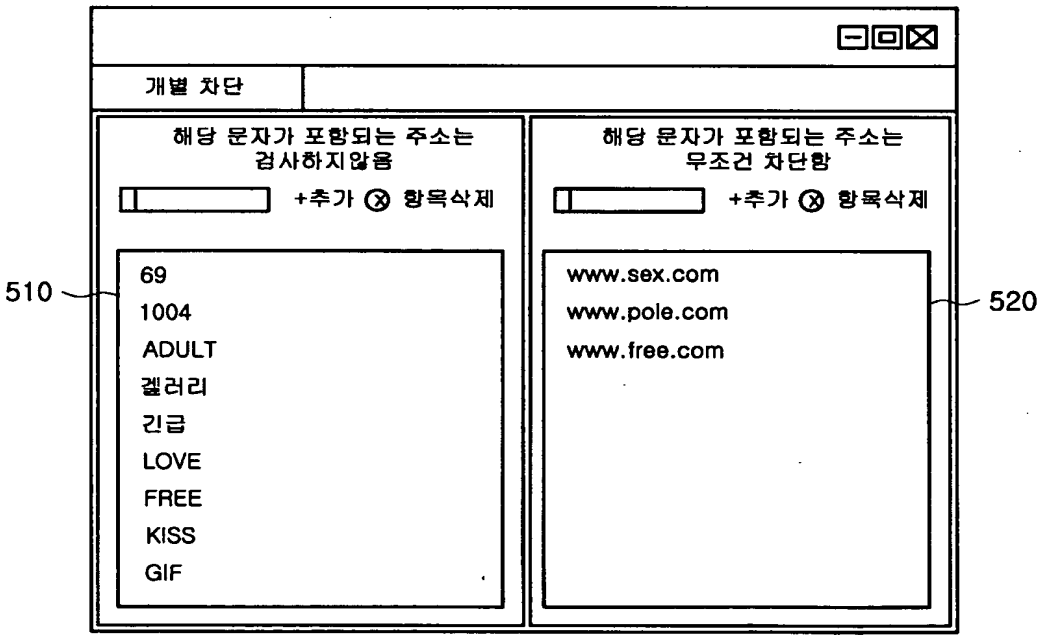
도면10


시 작
삭제
프로그램
추가/삭제
S51
추가
선택프로그램 지정/삭제
S56
제한할 프로그램 지정/추가
S52
S58
NO
더 삭제?
S57
Yes
NO
더 추가?
S53
Yes
S54
정보 설정 확인
S55
종 료

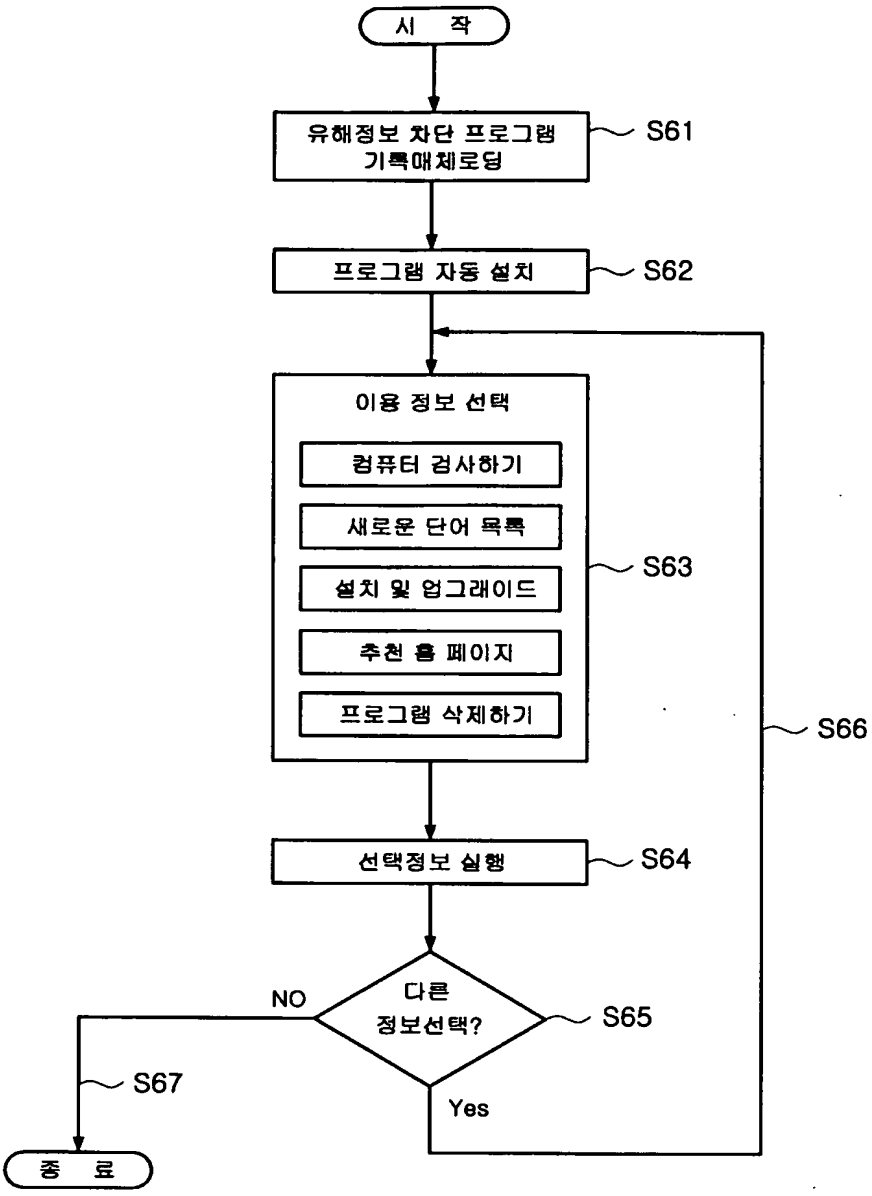
도면11


410
프로그램제한시간
인터넷 사용제한
420
일 월 화 수 목 금 토
1시 가능 금지 금지 금지 금지 금지 가능
2시 금지 금지 금지 금지 금지 금지 가능
3시 금지 금지 금지 금지 금지 금지 금지
4시 금지 금지 금지 금지 금지 금지 금지
5시 금지 금지 금지 금지 금지 금지 금지
23시 가능 가능 가능 가능 가능 가능 가능
24시 가능 금지 금지 금지 금지 금지 가능

도면12


개별 차단
해당 문자가 포함되는 주소는
검사하지않음
+추가
항목삭제
69
1004
ADULT
겔러리
긴급
LOVE
FREE
KISS
GIF
510
해당 문자가 포함되는 주소는
무조건 차단함
+추가
항목삭제
www.sex.com
www.pole.com
www.free.com
520

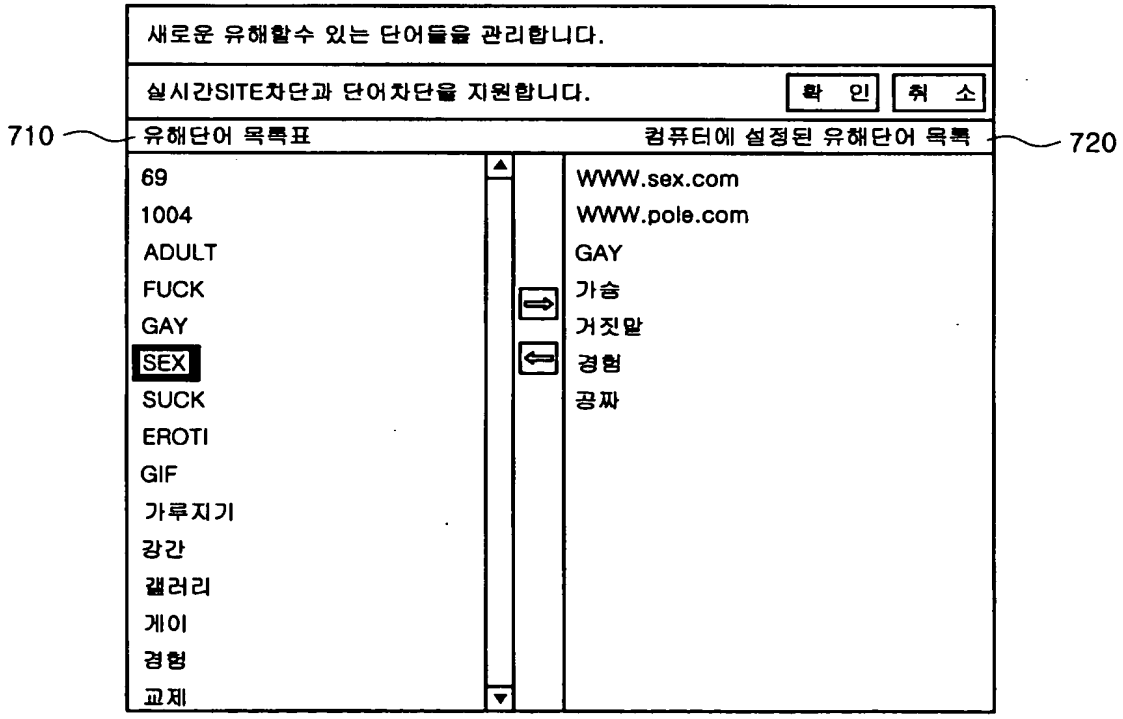
도면13


시 작
유해정보 차단 프로그램 기록매체로딩
S61
프로그램 자동 설치
S62
이용 정보 선택
컴퓨터 검사하기
새로운 단어 목록
설치 및 업그래이드
추천 홈 페이지
프로그램 삭제하기
S63
S66
선택정보 실행
S64
다른 정보선택?
S65
NO
Yes
S67
종 료

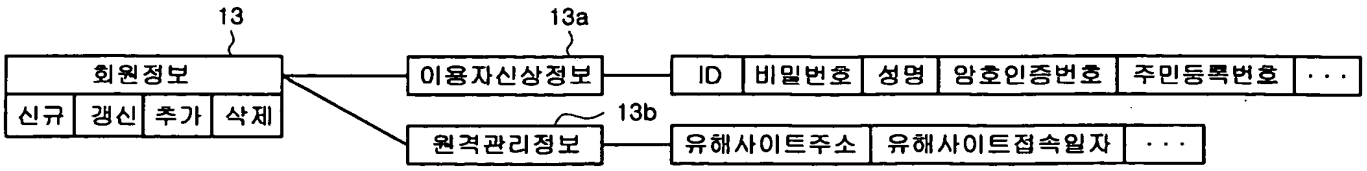
도면14


유해정보 차단 설정 프로그램
컴퓨터 검사하기
옵션 선택
하드 디스크선택
C:₩
D:₩
630
검사화일종류
*.BMP
*.JPG
*.JPEG
*.GIF
*.WMF
*.ICO
*.AVI
*.RA
630
검사시작
현재 검사위치: C:₩WINDOWS₩HLPSTEP3.GIF
630
C:₩SUHDLOG.DAT
C:₩WINDOWS₩BACKGRND.GIF
C:₩WINDOWS₩CLOUD.GIF
C:₩WINDOWS₩CONTENT.GIF
C:₩WINDOW₩HLPBELL.GIF
C:₩WINDOWS₩HLPCO.GIF
C:₩WINDOW₩HLPGLOBE.GIF
C:₩WINDOWS₩HLPLOGO.GIF
C:₩WINDOWS₩HLPSTEP1.GIF
C:₩WINDOWS₩HLPSTEP2.GIF
C:₩WINDOWS₩HLPSTEP3.GIF
C:₩WINDOWS₩TNLOGO.GIF
C:₩WINDOWS₩JAUTOEXP.GIF
C:₩WINDOWS₩HWINFO.DAT
C:₩WINDOWS₩SYSTEM.DAT
C:₩WINDOWS₩HH.DAT
C:₩WINDOWS₩98ESTUP.BIN
C:₩WINDOWS₩SUBACK.BIN
640

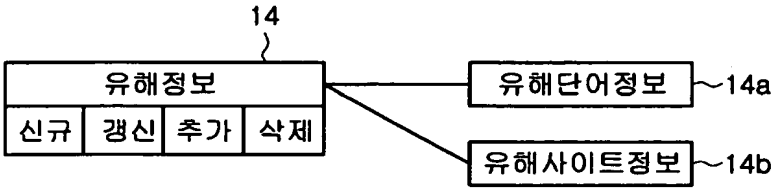
도면15


새로운 유해할수 있는 단어들을 관리합니다.
실시간SITE차단과 단어차단을 지원합니다.
확 인
취 소
710
유해단어 목록표
컴퓨터에 설정된 유해단어 목록
720
69
1004
ADULT
FUCK
GAY
SEX
SUCK
EROTI
GIF
가루지기
강간
갤러리
게이
경험
교제
WWW.sex.com
WWW.pole.com
GAY
가슴
거짓말
경험
공짜

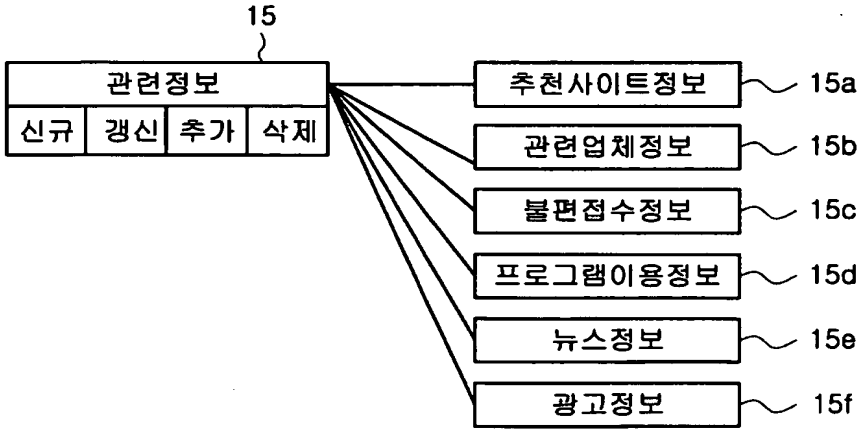
도면16


13
회원정보
신규
갱신
추가
삭제
13a
이용자신상정보
ID
비밀번호
성명
암호인증번호
주민등록번호
· · ·
13b
원격관리정보
유해사이트주소
유해사이트접속일자
· · ·

도면17


14
유해정보
신규
갱신
추가
삭제
유해단어정보
14a
유해사이트정보
14b

도면18


15
관련정보
신규
갱신
추가
삭제
추천사이트정보
15a
관련업체정보
15b
불편접수정보
15c
프로그램이용정보
15d
뉴스정보
15e
광고정보
15f

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox